UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/993,724	11/14/2001	Adrian Filipi-Martin	032121.00006 (CHM01)	9442

7590   06/10/2005

FLINT & KIM, P.A.
Douglas W. Kim
P.O. Box 10827
Greenville, SC 29601

EXAMINER
CHEN, SHIN HON

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 06/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/993,724	FILIPI-MARTIN ET AL.
	Examiner	**Art Unit**	
	Shin-Hon Chen	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _12 April 2002_.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
   closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-29_ is/are pending in the application.

     4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-29_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _14 November 2001_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

     a)☐ All   b)☐ Some * c)☐ None of:

       1.☐ Certified copies of the priority documents have been received.

       2.☐ Certified copies of the priority documents have been received in Application No. _____.

       3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
       application from the International Bureau (PCT Rule 17.2(a)).

     * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
   Paper No(s)/Mail Date _11/14/01_.

4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____ .

DETAILED ACTION

1.   Claims 1-29 have been examined.

Claim Rejections - 35 USC § 103

2.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

3.   Claims 1, 3, and 9-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Price, III U.S. Pat. No. 6851049 (hereinafter Price) in view of Mandelbaum et al. U.S. Pat. No.

5552897 (hereinafter Mandelbaum).

4.   As per claim 1, Price discloses a computerized system for encrypting an electronic

message between a sender and a recipient regardless of whether the sender or recipient are

members of an encryption system comprising: a computer processor; a computer readable

medium in communications with said computer processor (Price: column 2 line 12 – column 3

line 14); a communications link for communications between said computer readable medium

(Price: column 2 line 12 – column 3 line 14), a sender's terminal and a recipients terminal (Price:

column 2 line 12 – column 3 line 14); a set of non-member computer readable instructions

contained within said computer readable medium, when processed by a computer processor and

in response to a member sending an electronic message to a non-member recipient from said

sender terminal (Price: column 2 line 12 – column 3 line 14), generating an encryption key pair,

encrypting the electronic message responsive to said encryption key pair so that said key pair

may be used to decrypt said encrypted message (Price: column 2 line 12 – column 3 line 14),

sending a notification to said recipient terminal that an encrypted message is available to the

non-member recipient (Price: column 2 line 12 – column 3 line 14), encrypting said encryption

key pair according to said encryption pass-phrase (Price: column 2 line 12 – column 3 line 14),

decrypting said encrypted key pair in response to receiving a decryption pass-phrase

corresponding to said encryption pass-phrase (Price: column 2 line 12 – column 3 line 14),

decrypting said encrypted message according to said encryption key pair (Price: column 2 line 12

– column 3 line 14), and, providing the decrypted message for review to said non-member so that

the non-member can receive and decrypt an electronic message from a member of an encryption

system even though the non-member is not a member of the encryption system (Price: column 2

line 12 – column 3 line 14). Price does not explicitly disclose prompting the member for an

encryption pass-phrase at said sender terminal, receiving an encryption pass-phrase from the

member at said sender terminal and prompting the non-member for a decryption pass-phrase

corresponding to said encrypted message at said recipient, receiving said decryption pass-phrase

from the non-member. However, Mandelbaum discloses prompting sender and recipient for

encryption/decryption pass-phrase when communicating messages (Mandelbaum: column 4 lines

8-65 and column 7 lines 6-29). It would have been obvious to one having ordinary skill in the art

to allow sender and recipient to communicate messages using previously established keys stored

in a device carried by the users. Therefore, it would have been obvious to one having ordinary

skill in the art at the time of applicant's invention to combine the teachings of Mandelbaum

within the system of Price because it reduces processing power on central key management

servers when the recipient's key information is not stored in the key management server.

5.   As per claim 3, Price as modified discloses the system of claim 1. Price as modified

further discloses the system including: a member database contained within said computer

readable medium having a member record associated with each of the members of the encryption

system (Price: column 2 line 12 – column 3 line 14); a set of member location instructions

contained within said computer readable medium for: querying said member database for

determining whether the recipient has an associated record within said member database (Price:

column 2 line 12 – column 3 line 14), and, executing said non-member instructions if no

associated record is found for the recipient in said member database (Price: column 2 line 12 –

column 3 line 14 and Mandelbaum: column 4 lines 8-65 and column 7 lines 6-29).

6.   As per claim 9, Price as modified discloses the system of claim 1. Price as modified

further discloses the system including: a member database contained within said computer

readable medium having a member record associated with each of the members of the encryption

system (Price: column 2 line 12 – column 3 line 14); a unique public key contained within said

member record associated with each of the members of said encryption system (Price: column 2

line 12 – column 3 line 14); and, a set of reply instructions contained with said computer

readable medium in response to receiving a reply command from the non-member recipient

through said recipient terminal for: receiving a reply message from the non-member recipient

intended for the sending member (Price: column 2 line 12 – column 3 line 14); retrieving said

unique public key associated with the sending member from said member database (Price: column 2 line 12 – column 3 line 14); encrypting said reply message according to said unique public key of the sending member (Price: column 2 line 12 – column 3 line 14); and, informing said sending member that an encrypted reply message from the non-menber is available for decrypting and review by the member so that a non-member can send an encrypted reply to a member of an encryption system without having to be a member of that encryption system (Price: column 2 line 12 – column 3 line 14).

7.   As per claim 10, Price as modified discloses the system of claim 1. Price as modified further discloses the system including: a member database contained within said computer readable medium having a member record associated with each of the members of the encryption system (Price: column 2 line 12 – column 3 line 14); a unique private key contained within said member record associated with each of the members of the encryption system (Price: column 2 line 12 – column 3 line 14); a set of member instructions contained within said computer readable medium in response to a first member sending an electronic message to a second member for: retrieving a second member's public key from said member database, encrypting said electronic message responsive to said second member's public key (Price: column 2 line 12 – column 3 line 14); and, sending a notification to the second member notifying the second member that an encrypted message is available for decryption so that an electronic message is encrypted automatically and the receiving member is notified automatically when an encrypted message is available for decryption and review (Price: column 2 line 12 – column 3 line 14).

8.   As per claim 11, Price as modified discloses the system of claim 10. Price as modified

further discloses wherein said member instructions include instructions in response to the second

member requesting to decrypt the encrypted message for: retrieving a second member's private

key from said member database (Price: column 2 line 12 – column 3 line 14); decrypting the

encrypted electronic message from the first member according to said second member's private

key (Price: column 2 line 12 – column 3 line 14); and, providing said decrypted electronic

message to the second member for review so that an electronic message can be encrypted, sent

from a first member to a second member, and decrypt automatically (Price: column 2 line 12 –

column 3 line 14).

9.   Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Price in view of

Mandelbaum and further in view of Finkelstein et al. U.S. Pat. No. 5410602 (hereinafter

Finkelstein).

As per claim 2, Price as modified discloses the system of claim 1. Price as modified does not

explicitly disclose wherein said set of non-member instructions includes instructions for:

removing said unencrypted key pair from said computer readable medium; and, removing said

encryption pass-phrase from said computer readable medium so that only said encrypted

encryption key pair is contained within said computer readable medium. However, Finkelstein

discloses removing temporarily stored session key after it is no longer needed by the

infrastructure communication center (Finkelstein: column 4 lines 33-62). It would have been

obvious to one having ordinary skill in the art to delete the temporarily obtained key information

including session key and public key of recipient immediately after use because data processing systems have memory storage for storing temporary key information. Therefore, it would have been obvious to one having ordinary skill in the art to combine the teachings of Finkelstein within the combination of Price-Mandelbaum because it improves the overall security of the system by eliminating the possibility that someone could get unauthorized access to the key information.

10. Claims 4, 6, and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Price in view of Mandelbaum and further in view of Leonard et al. U.S. Pat. No. 6721784 (hereinafter Leonard).

11. As per claim 4, Price as modified discloses the system of claim 1. Price as modified does not explicitly disclose wherein said non-member encryption instructions includes instruction for: prompting the member at said sender terminal for a message lifetime value; associating said message lifetime value with the encrypted message send by the member; and, a set of lifetime deletion instructions contained within said computer readable medium for deleting said encrypted message upon expiration of said lifetime value associated with the electronic message so that upon expiration of said lifetime value the electronic message can not be decrypted and therefore is unavailable for review. However, Leonard discloses these limitations (Leonard: column 9 lines 11-61). It would have been obvious to one having ordinary skill in the art to set expiration time for the message by the sender. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of

Leonard within the combination of Price-Mandelbaum because it allows the sender to control the

processing the message.

12.   As per claim 6, Price as modified discloses the system of claim 1. Price as modified does

not explicitly disclose the system including a set of stale message instructions contained within

said computer readable medium for deleting said encryption key pair associated with said

encrypted message upon the expiration of a predetermined period of time so that if the encrypted

message is not decrypted within said predetermined period of time, the encrypted message is

unavailable for review. However, Leonard discloses these limitations (Leonard: column 9 lines

11-61). It would have been obvious to one having ordinary skill in the art to set expiration time

for the message by the sender so that is can be deleted/erased when time expires. Therefore, it

would have been obvious to one having ordinary skill in the art at the time of applicant's

invention to combine the teachings of Leonard within the combination of Price-Mandelbaum

because it allows the sender to control the processing the message.

13.   As per claim 7, Price as modified discloses the system of claim 1. Price as modified does

not explicitly disclose wherein: said non-member instructions include instruction for: prompting

the member at said sender terminal for a message lifetime value, associating said lifetime value

with the encrypted message sent by the member, and, a set of lifetime deletion instructions

contained within said computer readable medium for deleting said encryption key pair upon

expiration of said lifetime value associated with the electronic message so that upon expiration of

said lifetime value the electronic message can not be decrypted and therefore is unavailable for

review. However, Leonard discloses these limitations (Leonard: column 9 lines 11-61). It would

have been obvious to one having ordinary skill in the art to set expiration time for the message

by the sender so that is can be deleted/erased when time expires. Therefore, it would have been

obvious to one having ordinary skill in the art at the time of applicant's invention to combine the

teachings of Leonard within the combination of Price-Mandelbaum because it allows the sender

to control the processing the message.

14.   Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Price in view of

Mandelbaum and further in view of Doonan et al. U.S. Pat. No. 6807277 (hereinafter Doonan).

15.   As per claim 5, Price as modified discloses the system of claim 1. Price discloses

generating identifier and encrypted session key for each recipient (Price: column 2 lines 23-38)

Price does not explicitly disclose the system including: a message database included within said

computer readable medium having a message record associated with the electronic message; and,

said non-member instructions including instructions for: creating a message ID associated with

said electronic message to be sent to the non-member, storing said message ID within said

message record associated with the electronic message, and, storing said encrypted encryption

key pair within said message record associated with the electronic message. However, Doonan

discloses storing the key information and retrieval information after the keys have been

established (Doonan: column 2 lines 1-21). It would have been obvious to one having ordinary

skill in the art to store the encrypted key information and identifier associated with the recipient

into the storage location. Therefore, it would have been obvious to one having ordinary skill in

the art at the time of applicant's invention to combine the teachings of Doonan within the

combination of Price-Mandelbaum because it allows the sender to obtain useful information

regarding messages that were sent out.

16.   Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Price in view of

Mandelbaum and further in view of Anderson U.S. Pat. No. 6442600 (hereinafter Anderson).

17.   As per claim 8, Price as modified discloses the system of claim 1. Anderson as modified

does not explicitly disclose including deletion instructions contained within said computer

readable medium for deleting said encryption key pair upon receiving a delete request from the

non-member so that the non-member can expressly request the encrypted message be made

unavailable for review. However, Anderson discloses notify the recipient when message is

available and recipient can request the message to be deleted when it is no longer needed

(Anderson: column 2 lines 2-23). It would have been obvious to one having ordinary skill in the

art to allow recipient to request deletion of encrypted message because mail-processing system

can manage the messages being communicated. Therefore, it would have been obvious to one

having ordinary skill in the art to combine the teachings of Anderson within the combination of

Price-Mandelbaum because it enables recipients to control existence of the message.

18.   As per claim 12-29, claims 12-29 encompass the same scope as claims 1-11. Therefore,

claims 12-29 are rejected based on the same reasons set forth in claims 1-11.

Conclusion

19.   The prior art made of record and not relied upon is considered pertinent to applicant's

disclosure.

Ballard U.S. Pat. No. 6847719 discloses preventing receivers from decrypting a

encrypted message when the encrypted message is expired.

Cook et al. U.S. Pub. No. 20040139314 discloses selecting different mode of delivery for

electronic messages.

Marvit et al. U.S. Pat. No. 6625734 discloses controlling and tracking access to

disseminated information.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Shin-Hon Chen whose telephone number is (571) 272-3789. The

examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shin-Hon Chen
Examiner
Art Unit 2131

6|9|05

SC